Exhibit 6

Excerpts of SW-SEC00001551

solarwinds

SECURITY & COMPLIANCE PROGRAM QUARTERLY

NOVEMBER 15, 2019

DEVELOPMENT, OPERATIONS & INFORMATION TECHNOLOGY (DOIT)

SolarWinds Scorecard

NIST Maturity Level

Security Category	2017	2018	2019
Identify	0.8	2.0	3.0
Protect	1.5	3.0	3.2
Detect	1.0	2.8	3.6
Respond	0.8	2.8	3.6
Recover	0.7	2.0	2.0
Overall	1.0	2.5	3.1

Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measure its compliance
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost effective manner

INDENTIFY

Highlights

- Instituted standardized security scoring method (CVSS). 421 internally discovered issues marked security | 292 resolved in 1H 2019
- Open Source License Scanning coverage across entire portfolio
- Full lifecycle software asset management
- ISO certifications achieved for RMM, Backup, Take Control. N-central, Mail Assure (In progress), SOC 2 Type 1 for Passportal, Loggly & App Optics (in progress)
- Threat intel ingestion remains a manual process

Security Category	Objective	NIST Maturity Level
Asset Management	Internally and externally facing assets are identified and actively managed	**3**
Secure Software Development Lifecycle (SSDL)	Employees are aware of an utilize a security software development lifecycle in their day to day activities	**2**
Open Source License Scanning	Open source code used is scanned and remediated as needed	**3**
Product Certifications	ISO 27001 information security management system (ISMS) framework of policies and procedures are followed and audited annually	**3**
NIST internal program assessment	The internal security program and practices are aligned with NIST	**3**
Vendor Management / Procurement	Vendor management and procurement practices include security reviews for each asset	**5**
	Identify Maturity Level	**3.2**

PROTECT

Highlights

- Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures
- Comprehensive firewall protection for Corporate IT and web properties (Palo Alto Next Gen firewalls in place (58) | Web Application Firewalls (WAF) on all key marketing properties)
- Improved end point protection. End user devices coverage: 80% SEP | 85% encryption | 95% DLP. IT servers coverage: 91% SEP. Hosted environment assessment WIP
- Moving towards Zero Trust model (where we loosely protect all and strongly protect those that can-do material harm). Less requirements on VPN
- Spam / Phishing still a challenge. Adversaries are getting better. Increase in whale phishing (55 million messages blocked 1H2019)
- Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets
- Additional monitoring via SOC is planned for 2nd half of the year

Security Category	Objective	NIST Maturity Level
Next Generation Firewalls	Palo Alto Firewalls are deployed and actively monitored across the company	**5**
Web Application Firewalls	WAFs are deployed for marketing properties but not for production products	**3**
Endpoint Protection and Encryption	Endpoint protection and encryption is deployed and actively managed across the company	**4**
Data Leakage Protection	Data leakage protection is deployed across the company and actively monitored	**3**
Spam / Phishing Detection / Response	Email protections are in place to monitor spam, detect phishing and deter known email scammers	**3**
Authentication, Authorization and Identity Management	User identity, authentication and authorization are in place and actively monitored across the company	**1**
	Protect Maturity Level	**3.2**

RECOVER

Highlights

- Recovery for basic incidents managed well
- Differencing DR/BCP level of capabilities per product, datacenter region
- Need to model major events and define necessary data to appropriately perform forensics

Security Category	Objective	NIST Maturity Level
Backup and Recovery Program	Across SolarWinds products and other mission critical assets, a backup and recover plans are in place	2
Disaster Recover / Business Continuity Program	Across SolarWinds products and other mission critical assets, disaster recovery and business continuity plans are in place	2
Forensics Program	A forensics program is established and actively managed within the company	2
	Recover Maturity Level	**2.0**